Global Information Assurance Certification Paper

Brian Zaiser
SANS Security Essentials
GSEC Practical Assignment, Version 1.4b Option 2
2004 April 12

Making the Right Moves – Improving the Security "Posture" of a Smaller Company

Abstract

Many smaller companies realize the importance of keeping their data secure but may not realize how many very simple methods can be used or vulnerabilities can be taken advantage of to obtain sensitive information. Sometimes concerns about 'productivity' (and cost) overshadow concerns about security, at least until an incident or incidents occur (possibly affecting the reputation of the company) to shift focus.

I worked for a smaller manufacturing company that, at one time, would have been considered reasonably secure. Due to an embarrassing incident, focus shifted to electronic data security, and the IT staff. Demands for improving security and computing applications increased, we needed to re-examine practices and policies as well as our network infrastructure and configurations.

The balancing act of cost, productivity and security plays out differently for each company. It can hamper security efforts or security can hamper productivity. Most computer programmers and network administrators are not security experts and cannot dedicate themselves to only one project. There were only two of us to meet all the computing needs of the company. Don MacVittie speaks of how difficult this becomes in his piece "Don't Drive Your Security Staff Nuts"[1] in which he posits that "we've asked them to not only be jacks of all trades, but masters of all trades too". The combination of this and other factors can lengthen the process, to the extent that, sometimes, not all persons involved in the process can see it to 'completion' (as happened to me).

'Completion' is not actually an appropriate term. Maintaining security is always a continuing and evolving process. George V. Hulme states: "Last year was a bad one for information-security professionals. This year is likely to be even worse."[2] There is no "silver bullet". However, progress was made and a sound course was set. This partly through trial and error as I had not yet had training from SANS. This is a review (partly) of what happened in light of my later training.

Before

Status quo

[1] Don MacVittie. "Don't Drive Your Security Staff Nuts"
[2] George V. Hulme. "Security Threats Won't Let Up This Year"

When I started working for this particular employer, there were two LAN administrators, because there were two LANs – one for one department and another for the rest of the company. The two networks were not connected. The network hardware used was different (hub v switches, BNC v RJ45); the physical network topologies were different (bus v star); the user ID scheme was different; the password policy was different (stated v "understood"); the anti-virus software was different and the update policy was different.

It wasn't a question of not being able to connect those machines, the cables were run, there was space on the server, almost all of the network cards in the department had both connectors, etc. The issue was the policy adopted by each administrator and their supervisors.

The department's network was rather secure: it did not connect to the outside world except on rare occasions using a modem on selected machines and the administrator sometimes connecting to the corporate LAN; software was "not allowed" to be installed without approval; the anti-virus software was updated semi-regularly. The administrator accomplished this by disconnecting from the department's network and plugging in to the corporate network, downloading the new virus definition file and performing an update by walking from machine to machine. One security concern was the choice of operating systems. Each desktop dual booted into either Windows98 or Windows NT 4.0 because the application used for the old drawing files was a DOS application and ran better under Windows98. The newer drawings used a newer application run under Windows NT 4.0 Workstation.

I was concerned about the fact that Windows98 was installed on corporate machines, because I knew that, generally speaking, all versions of Windows 3.x and 9x were less secure than Windows NT. I didn't realize, until after attending SANS, how great a risk this posed. Even the Windows NT machines posed a problem. For backward compatibility, a DOS networking component was included in Windows 9x and Windows NT 4.0. This component breaks the passwords into two segments of seven characters (max) each and converts all letters to upper case, making a crack much easier[3]. Once the passwords are cracked, unauthorized access can be gained to other systems and their data. We knew that these machines would eventually be added to the corporate LAN.

The corporate network was less secure. Not only was virtually every machine connected to the Internet, but also almost every system had instant messenger software installed, which leaves ports open that are often used for attacks. Almost all the systems had anti-virus software installed, but it wasn't very up-to-date and it wasn't the same version from machine to machine. There were different operating systems resulting in different inherent security levels and not all the machines were up-to-date in operating system patches. One other security

[3] Eric Cole, et al. p. 423

concept that *was* implemented – using private TCP/IP address numbers for inside and inward facing network cards, and using the "real" corporate IP address only for the server's outward facing network card.

There was no written policy or procedure for updating anti-virus software and operating systems nor hardware drivers. Almost no one who had the ability (and, therefore, greater need) to update the software really understood how or why; and no one enforced the updates. The updates were not automatic, even the machines set to do 'automatic' updates weren't updating. The updates were not pushed from the server, either. We didn't know how to accomplish this.

What prompted a change?

One morning, I received an email from someone within the company with whom I usually had very little interaction. It seemed quite odd that I would receive joke email from him. Before I could open it, there were three more copies in my inbox from the same person.

I immediately suspected a virus and said so as I watched multiple copies of the exact same message arrive from other unlikely senders in addition to the first sender. My supervisor was not convinced. It was only after five or six more people started sending multiple copies (and perhaps trying to open the attachment himself) that my supervisor recognized that it was indeed a virus and time to do something.

As soon as I had advised my supervisor, I started looking for the name and solution to this virus. I found the necessary information and forwarded it to my supervisor who then tested the solution on his own machine, printed it out and we then began circulating to clean up the mess.

The company was brought to a standstill. So were we, or nearly. To avoid public relations difficulties, we didn't use the intercom system to advise people not to open any of the messages. However, the phone kept ringing with people saying, "I can't open this message."

People were shocked to learn that it was a virus and that they kept spreading it each time they tried to open it. They weren't very happy either to be told to "be patient", we would get to them, eventually.

Of course, the obvious fallout was immediate. Upper management was confused and concerned. How could this have happened? How can we prevent it from ever happening again? Weren't we doing our job?

The first step was the blame game. It was pointed out that individuals were responsible for their own machines. Users complained that they didn't know how to perform updates. Or, they thought it was automatic. They were told that they

had been shown on various occasions. They said they forgot and it wasn't made clear why they needed to update the software, nor why it should fall to them. Shouldn't it be automatic? Wasn't it the IT department's job?

On a directive from management, we were to improve the general security "posture" of the company. For most people, this means only hardware and software updates, but really, it includes physical security and user attitude and awareness. We tried to take a holistic approach, examining the problem and goal piece by piece.

Investigation showed how far behind most machines really were, and that some didn't even have anti-virus software installed or running, not just that it wasn't up-to-date. (When asked why he had disabled the anti-virus software on his machine, one person replied that he didn't understand the annoying message that popped up now and then, didn't know what to do about it, and wasn't going to bother us with it. Although it remained unspoken, the suspicion was that this may have been related to the content this person was expecting, as opposed to the actual payload and he didn't want to be caught with either the expected content or the payload.) It was obvious that some "retraining" was necessary and that other solutions should be investigated.

Operating systems also needed significant updates. Some were two service packs behind. Not only did user machines need updates, but also the servers needed them. This was, of course, mainly because there was only one server (at the time), and it was not desired to shut down the server to perform updates, even after hours. Even after adding another server, it wasn't desired to shut down either as they performed separate vital functions.

The anti-virus protection on the server wasn't adequate. It was an older version that wasn't being kept up-to-date. It didn't integrate well with either the email server or the proxy server.

Firewall capability was a component of the server software. My supervisor managed this. The software kept logs; but the logs weren't checked very often because there were *many* entries showing unauthorized (but as far as we knew, unsuccessful) attempts to connect through various ports. It appeared to be working well, but we thought a port scan would be worth the effort.

By searching the Internet, we discovered a web site that offered to do a port scan for free. (Several sites are available: Audit My PC at http://www.auditmypc.com, Security Metrics at http://www.securitymetrics.com/portscan.adp, Broadband Reports.com at http://www.dslreports.com/scan, et al.) The site said that the scan would likely be ineffective if a firewall was active. We tried anyway and were surprised how many ports were still scanned through the firewall (indicating a configuration problem), but many more reported an inability to be scanned because of the firewall. It was necessary to use a different tool that ran locally

and we were surprised to find how many of these other ports were still open. The tool also showed which services commonly use which ports. After seeing which ports were open and which services correspond to them, we went through the list of services to determine which were needed.

Another need for change was the desire to move more processes to computer and have interoperability among the applications. This necessitated adding more PC's and therefore more network equipment. Also, the LAN administrator for the separate department left and that department was soon to be added to the corporate LAN as well.

We were not completely ignorant about implementing security measures. We had some sense of how to improve, but we weren't sure how to accomplish some and unaware of the rest.

Even before the attack and restructure, I had accessed online periodicals at my previous workplace and subscribed as soon as I had access. Newsletters from SANS and Network Computing topped my list. I also made it a priority to be on lists for notification, from the software vendor, of virus outbreaks. My supervisor introduced me to the concept of Windows Updates online and not needing to get CDs for service packs. We attended Microsoft's one-day lecture on machine and network security to learn about some of the utilities available.

During

Network

As the need for network availability increased, we considered what equipment would best provide. Since Ethernet equipment was already being used, is faster and less expensive than token ring, there was only one choice. Obviously, we did not want to use hubs but switches because switches keep tables of what addresses map to which ports and can route packets directly to the intended segment and reduce broadcasting, and therefore, collisions and the possibility of packet sniffing. As we would be installing computers in other buildings, we decided to use optic fiber to extend the LAN to these buildings since there is a limit on the distance for Cat 5 wiring. By segmenting the network and keeping department wires grouped together, we are better able to track down problem areas and manage the overall network.

We already had 10BaseT switches but needed to upgrade. We purchased a fiber switch and connected each server and building to this switch. We also purchased 100BaseT switches, and fiber adapter cards for a switch in each building. This was a potential bottleneck as only each building, not each switch (three in one building) connected to the fiber switch and, thereby, the servers; however, cost was becoming an issue. We reused one 10BaseT switch for the one department

because the network demands were much less: retrieving drawings and occasional email. Another was saved as a backup in case of failure.

Servers

When I started, there was only one server with six disks, only five in a RAID array. The separate drive did fail; but, fortunately, only one department was affected (but visibly) and most of the information was recovered. This demonstrated the importance of RAID. When we restructured, we now had two servers, each to perform separate functions – one for communications and authentication, the other as a file and data server. Each used RAID arrays to allow for data recovery. In case a disk failed again, that disk would be replaced and the data would be recreated by the array.

It was decided that, as the current operating system would have no further patches, it was necessary to upgrade to the next version. The decision was made not to skip to the latest version because of cost and concern about reliability and security, as it had not been available for more than a year, allowing time for the first major patches to be released. New versions of some existing software needed to be purchased, including the anti-virus software, which now integrated with the mail and web proxy server software.

Firewall functionality was a component of the server software in this version as well. Again, my supervisor managed this.

We ran the port scanner against the newly configured outward facing server. The report showed that there were still several ports open by default. Using the report from the port scanner, we determined the ones that weren't needed and, eventually, closed them.

Under the old version of the server software, we had divided users into user groups and allowed access both to the files and directories and services based on those groups and sometimes based on user. We encountered a problem based on rights assignments because a user used the "Take Ownership" checkbox on the properties page of some files and blocked access to other users. We quickly corrected that problem and kept it under consideration when we restructured. As more people, and user groups, were added, we needed to reconsider who needed what kind of access to services and directories. It took longer than we thought, but we managed to work it out.

I had been reading articles in Network Computing about DMZ's, or demilitarized zones[4]. I discussed DMZ's with my supervisor as a possible measure to secure our systems further. After some discussion, we decided that it wasn't feasible because of the amount of money needed for additional hardware. The topic of honeypots was also broached, but considering that hardware was an issue, and

[4] Brooke Paul. "Building an In-Depth Defense"

that there are security concerns if ever the protections used in implementing a honeynet failed, my supervisor quickly abandoned the idea.

The email server software was configured for each user as that user was added to the domain. Some users had some kinds of attachments blocked. There are, though, ways to circumvent this.

Workstations

As more employees joined the company or needed access, new machines were purchased and machines moved around in accordance with need. Each machine was built/rebuilt as needed and a later version of the operating system installed for security. Some machines had the CD-ROM and floppy drives removed for added security, but also for "productivity". Concerns about playing games and installing software seemed to be addressed by the removal of drives, however, these people also had email and could install software sent as attachments.

Almost all employees now would have email and would therefore need anti-virus software. The new version allowed a client set-up for users without internet access. This allowed for patches to be downloaded to the server and pulled by the clients when users logged on. Users with internet access were still responsible for performing updates themselves and were shown how to accomplish this.

Physical Security

During my first few months, the server was in the office I shared with my supervisor. Our door was always open and not lockable. Anyone, at any time could easily walk in and pull the plug or turn off the server. The hard drives were locked in place and the key was kept in a different department. This provided some physical security. Of course, the fact the plug could be pulled represented a greater risk. (A reflection on data concerns is evident in the fact that our 'department' was called Data Processing and fell under the auspices of the Accounting Department.)

During our network restructure, we moved the server to a rack in a locked room that had been built around the network switches. This provided one part of the physical layer in the defense-in-depth model espoused by SANS[5]. We purchased an uninterruptible power supply for the servers. The switches already had an uninterruptible power supply. Each PC had its own UPS; the laptops had batteries, which would take over if outlet power was lost. All this was to try to prevent corruption of data caused by power failure; power failure is not uncommon. However, not all the machines were correctly configured to save the data and shut down safely during a power failure.

[5] Ibid. Chap. 7.

Policy Changes

Even with these improvements, people's attitudes about security needed to change. This would be attempted by crafting policy. People would be aware of what behaviors were expected of them. Some changes would be made.

Passwords are often weak, especially for those unconcerned with data security and more concerned about getting access quickly. This is often the weakest point in any security scheme, but usually the least expensive to change.

One department used an application that kept all the data on the server but also kept user-specific data on the individual laptops. The user controlled ownership of the data assigned to him. Sometimes, the ownership/assignment of the data needed to be changed when that user was not available. Therefore, most people in that department knew or could guess each other's passwords so they could login to that user's machine to change the "ownership". This issue was being addressed when I was laid off.

In another department, "only one" person had access to a desktop system. We learned later that others had been accessing that machine to do that person's work and using that person's password, which he had told them. In this case, we changed that user's password without notification and when he complained, we explained about the need for security and that if others needed to do the same job, they would need their own accounts either on that machine or on machines we would provide for them.

This demonstrates how important it is that, not only does "everyone" sign-off on ideas, but also everyone is "involved" in the process so that most eventualities are considered before making policy and needing to "fix" things later.

My supervisor and I crafted a new password policy to address the obvious weaknesses. I wanted to use more stringent guidelines, but my supervisor was more concerned about people's perception of how difficult it would be to come up with passwords and how easy they were to remember. The recommendation of SANS, et al. is to use at least eight characters from all four character sets - upper, lower, numeric and special (punctuation and/or <alt> symbols, e.g., <alt> 234 = •). (For a discussion, see the article by Raj Shekhar – "Choosing Strong Passwords")[6] We decided to enforce the length but using only (at least) three out of the four character sets. We agreed to keep some password history and to require changing more often, with a minimum age, but not so often, or so much history, that people were likely to complain and/or not comply. All passwords would be "submitted" for approval, (rather than trying to crack them), at least for the first time so people would get some practice. Passwords could not contain personally identifying information, nor words from the dictionary. People would be required to keep their password(s) secret and, if not, the password(s) would be

[6] Raj Shekhar. "Choosing Strong Passwords", NewsForge

changed and the person would be “retrained”. New employees were subject to this policy immediately, even before management “sign-off”. However, I was laid off before we received management write off for this to apply to everyone.

After

Network

We did have some networking problems after the restructure. One switch went bad and needed repairs. The fiber cable to one building had a break and data transmission was “spotty”. Fortunately, the break was at the connector and corrected by replacing the connector further back on the cable. Some workstations had trouble communicating, but that was an IP configuration problem on those systems and corrected quickly. Upon correct implementation of switches and workstation network configurations, broadcasting did decrease and it was easier to troubleshoot network connections.

Server

It took some reading and experimentation, including two rebuilds, but the servers ran well, seemed to be stable and blocked access as expected.

After the last install of the new version of the sever operating system, we ran the port scanning software again to find open ports. After determining what was not needed, we stopped unnecessary services and closed those ports and ran the test again to show that they were indeed closed. This did not seem to introduce any problems with access.

We used Access Control Lists and User Groups to grant and deny privileges to files and directories. There were no reported access-related difficulties.

As a small company, we did not have our own web server but relied on our ISP for access out, hosting the site, and some security of both that data and access to our server. We started to “publish” some data (email), which can open back doors. However, by auditing the various logs, we did not detect any intrusions.

As mentioned, the password policy was not yet implemented before I was laid off. Therefore, I am unaware of its being implemented (universally) or any “difficulties” it caused.

Physical Security

There were occasions that access to the network/server room was necessary - running the fiber cable to each of the other buildings, running telephone lines to that room, etc. Each time, unfortunately, the door was often left standing wide open and the equipment was often unattended (the room is in the basement, our

office was on the second floor). Fortunately, most of the employees knew enough not to touch anything, even if we asked them.

The uninterruptible power supplies for each workstation were eventually configured properly, although we learned later that some needed replacing. The UPS for the servers, however, was a different story. We still did not have a good understanding of its configuration before I left. I am not aware if this was solved.

Plans

Because of ease-of-use, data-integrity and accessibility issues with the application that stored some data on individual machines, the decision was made to rebuild the application from scratch so that users could access the data on the server directly through a web browser no matter where the user was. Eventually a third-party application was implemented after I was laid off.

We planned to move to the latest version of the server operating system; however, we wanted more information on it and some training (as well as allowing time for the first service pack). We also wanted to manage patches by "pushing" updates to the clients from the servers. I am unaware if these upgrades have been performed.

We wanted to continue moving all older systems from Windows98 to Windows2000. However, there were three impediments. First, not all of the older drawings had been converted from the DOS software's format and a couple of trusted individuals kept their dual-boot systems with the understanding they would be upgraded later. Second, personnel issues in another department made it desirable to management to access those systems directly and quickly (i.e., those users could not "lock" their desktops). Third, one system in that department used an interface card to connect to the mid-range through emulation software. The concern was finding another card or driver for Windows2000 and Windows98 had been difficult enough. I do not know the current status of user systems.

My supervisor had advised management of the necessity to replace the aging mid-range, which housed all of the company's accounting data and was not year 2000 compatible. Another department head had pushed for software he could use that would tie in to the accounting department. The company purchased and installed software that had been recommended and that other department began using it. This software did not exactly fit the needs or "business model/flow" of the company, but it was customizable. However, after several attempts, the accounting software was considered a "failure" and was to be replaced. As I had been hired to support the accounting software, and the decision was made to outsource much, if not all, future development, I was no longer considered a viable asset to the company and was laid off. I do not know the current status of the accounting software.

Such decisions are necessary, but can lead to even more security issues. User authentication and secure transmission become paramount in the use of any internet-based application. There should be concern of backdoors and other weaknesses in the code of any outsourced application (or outsourcing generally)[789]. The security level of the browser itself also becomes an issue.

Conclusions

When I started working at this company, I was amazed at the 'stance' with regard to data and workstation security. People made several assumptions and there was no verification and no enforcement of most policies and no one really seemed to care. With one email worm that almost paralyzed the company, focus shifted from 'lack-a-day' to reactive with IT trying to shift it further to 'pro-active'. We achieved this in some areas. In light of my SANS training, I would recommend even more changes or taking them further.

Obviously, I would upgrade all operating systems and software on servers and workstations to the latest versions with the latest (proven) patches and harden the machines. I would use automatic downloads of updates to the server and "push" them to the workstations. I would enforce longer, more complex passwords with more history, a longer minimum age and changing them more often. I would not use obsolescent technologies to track workstation network information (e.g., WINS, LMHosts, NetBIOS, etc.), but use DNS. I would enforce more frequent auditing of server and PBX logs. Because data is being "published" and accessed through web browsers, I would separate sensitive data and use a DMZ for such applications. I would make hardware upgrades to servers and network infrastructure to distribute loads and accommodate a DMZ. I would move the rack to a more central and accessible, yet secure and physically safe location with the IT office nearby. All IT personnel would have non-administrative level access accounts with access to a limited number of administrative accounts. All on-campus machines would use a properly configured UPS.

There are other steps that could be taken, but for a smaller company, the balancing act of security, cost and accessibility/ease-of-use usually favors cost and ease-of-use – until there's another incident.

Yes, one security event can trigger profound changes in a company's attitude and implementation of electronic data security. But, the changes can introduce new concerns either in being able to do one's job or other personnel issues. No, it is virtually impossible to see a comprehensive overhaul through to completion because, really, it never ends. The war rages on.

---

[7] Antone Gonsalves. "Overseas Outsourcing Leads To Identity Theft Risks".
[8] Rob Enderle. "The Other Side of Outsourcing: Dangers Offshore", ECommerceTimes.com.
[9] Phil Friedman. "Exec Outlines Perils Of Offshore Outsourcing", Information Week.

References

Hulme, George V.. “Security Threats Won’t Let Up This Year”, Network Computing. 05 January 2004. http://nwc.securitypipeline.com/showArticle.jhtml?articleId=17200247&printableArticle=true. (17 March 2004).

MacVittie, Don. “Don’t Drive Your Security Staff Nuts”, Network Computing. 21 August 2003. http://www.securitypipeline.com/showArticle.jhtml;jsessionid=DJX1MCPKCKJTMQSNDBGCKHY?articleId=13100919&printableArticle=true. (17 March 2004).

Shekhar, Raj. “Choosing Strong Passwords”, NewsForge. 26 February 2003. http://www.newsforge.com/article.pl?sid=03/02/26/1639212. (18 March 2004).

Cole, Eric; et al, SANS Security Essentials with CISSP CBK, Volume One, Version 2.1, copyright 2003, The SANS Institute, Chapter 7, pp. 292-331

Gonsalves, Antone. "Overseas Outsourcing Leads To Identity Theft Risks", Network Computing. 11 February 2004. http://nwc.securitypipeline.com/showArticle.jhtml?articleId=17603278&printableArticle=true. (17 March 2004).

Enderle, Rob. “The Other Side of Outsourcing: Dangers Offshore”, ECommerceTimes.com. 20 April 2004. http://www.ecommercetimes.com/perl/story/32946.html. (20 April 2004).

Friedman, Phil. “Exec Outlines Perils Of Offshore Outsourcing”, Information Week. 24 September 2003. http://www.informationweek.com/story/showArticle.jhtml?articleID=15200264. (20 April 2004)

Paul, Brooke. “Building an In-Depth Defense”, Network Computing. 9 July 2001. http://www.networkcomputing.com/shared/printArticle.jhtml?article=/1214/1214ws1full.html&pub=nwc. (22 April 2004).